Interrogation écrite 2

Vendredi 21 novembre 2025, 11h15–12h45 (1h30)

Les documents et le matériel électronique sont interdits. Les exercices sont indépendants les uns des autres. Toutes les réponses doivent être justifiées. Le barème est indicatif.

1. Étudier l'irréductibilité sur $\mathbb{Z}$ des polynômes suivants :
   (a) $P_1 = 4X + 2$. 0,5 pts

> **Solution:** Le polynôme P_1 est **réductible** sur $\mathbb{Z}$. Le contenu de P_1 est $c(P_1) = \text{pgcd}(4, 2) = 2$. Puisque $c(P_1) \neq \pm 1$, P_1 n'est pas primitif. On a la factorisation $P_1 = 2(2X + 1)$. Les facteurs 2 et $2X + 1$ ne sont pas des unités dans $\mathbb{Z}[X]$ (les unités sont 1 et -1). P_1 est donc réductible.

   (b) $P_2 = X^3 + 2X^2 + X + 1$. 1 pt

> **Solution:** Le polynôme P_2 est **irréductible** sur $\mathbb{Z}$.
>
> 1. P_2 est **primitif** car $c(P_2) = \text{pgcd}(1, 2, 1, 1) = 1$.
> 2. D'après le lemme de Gauss, P_2 est irréductible sur $\mathbb{Z}$ si et seulement s'il est irréductible sur $\mathbb{Q}$.
> 3. P_2 est de degré 3. S'il était réductible sur $\mathbb{Q}$, il aurait nécessairement une racine dans $\mathbb{Q}$. Les seules racines rationnelles possibles sont ± 1.
>   — $P_2(1) = 1 + 2 + 1 + 1 = 5 \neq 0$.
>   — $P_2(-1) = -1 + 2 - 1 + 1 = 1 \neq 0$.
> P_2 n'a pas de racine rationnelle. Il est donc irréductible sur $\mathbb{Q}$, et par suite, sur $\mathbb{Z}$.
>   (*Alternative : La réduction mod 2, $\overline{P}_2 = X^3 + X + 1$, est irréductible sur $\mathbb{F}_2[X]$, donc P_2 est irréductible sur $\mathbb{Z}[X]$*).

   (c) $P_3 = X^4 + 2X^2 + 4$. 1 pt

> **Solution:** Le polynôme P_3 est **irréductible** sur $\mathbb{Z}$.
>
> 1. P_3 est **primitif** car $c(P_3) = \text{pgcd}(1, 2, 4) = 1$.
> 2. **Racines de degré 1 :** Posons $Y = X^2$. $Q(Y) = Y^2 + 2Y + 4$. Le discriminant est $\Delta = 2^2 - 4(4) = -12 < 0$. Q n'a pas de racines réelles, donc P_3 n'a pas de racines réelles, et par conséquent pas de racines rationnelles. P_3 n'a pas de facteur de degré 1.
> 3. **Factorisation de degré 2 :** On cherche une factorisation $P_3 = (X^2 + aX + b)(X^2 + cX + d)$ avec $a, b, c, d \in \mathbb{Z}$. L'identification des coefficients mène au

système :

$$X^3 : a + c = 0 \implies c = -a$$
$$X^0 : bd = 4$$
$$X^2 : b + d + ac = 2 \implies b + d - a^2 = 2$$

En analysant les cas pour $bd = 4$ (i.e., (b, d) est dans $(1, 4)$, $(4, 1)$, $(-1, -4)$, $(-4, -1)$, $(2, 2)$, $(-2, -2)$ ou une permutation) et en combinant avec la dernière équation, on trouve qu'il n'existe **aucune solution entière** pour a, b, d. Par exemple, si $b = d = 2$, $b + d - a^2 = 4 - a^2 = 2 \implies a^2 = 2$, impossible dans $\mathbb{Z}$.

(d) $P_4 = X^4 + 3X^3 + 2X^2 - 1$. 1,5 pts

Solution: Le polynôme P_4 est **irréductible** sur $\mathbb{Z}$.

1. P_4 est **primitif** car $c(P_4) = \text{pgcd}(1, 3, 2, -1) = 1$.
2. On étudie la **réduction mod 2** de P_4 :
$$\overline{P_4} = X^4 + X^3 + 0X^2 + 1 \in \mathbb{F}_2[X]$$
3. **Racines dans $\mathbb{F}_2$:** $\overline{P_4}(0) = 1 \neq 0$, $\overline{P_4}(1) = 1 + 1 + 1 = 1 \neq 0$. $\overline{P_4}$ n'a pas de facteur de degré 1.
4. **Facteurs de degré 2 :** Le seul polynôme irréductible de degré 2 sur $\mathbb{F}_2$ est $Q = X^2 + X + 1$. On vérifie si $\overline{P_4}$ est divisible par Q ou est égal à Q^2.
$$Q^2 = (X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq \overline{P_4}$$
En effectuant la division euclidienne de $X^4 + X^3 + 1$ par $X^2 + X + 1$ dans $\mathbb{F}_2[X]$, le reste n'est pas nul.
5. $\overline{P_4}$ est irréductible sur $\mathbb{F}_2$. Par le critère de réduction, P_4 est irréductible sur $\mathbb{Z}$.

2. On considère le polynôme $\Phi_5 = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Z}[X]$. On note $\zeta = e^{2i\pi/5}$ une racine primitive 5-ième de l'unité.

(a) Démontrer que la réduction mod 2 de Φ_5 (c'est-à-dire vu comme un élément de $(\mathbb{Z}/2\mathbb{Z})[X]$) est irréductible. 1 pt

Solution: Soit $\overline{\Phi_5} = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$.

1. **Absence de racines :** $\overline{\Phi_5}(0) = 1 \neq 0$ et $\overline{\Phi_5}(1) = 1 + 1 + 1 + 1 + 1 = 5 \equiv 1 \neq 0$. $\overline{\Phi_5}$ n'a pas de facteur de degré 1.
2. **Absence de facteurs de degré 2 :** Le seul polynôme irréductible de degré 2 sur $\mathbb{F}_2$ est $Q = X^2 + X + 1$. S'il était réductible, $\overline{\Phi_5}$ serait le produit de deux facteurs irréductibles de degré 2.
$$\text{Facteurs possibles} = Q^2 = (X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq \overline{\Phi_5}$$
Ainsi, $\overline{\Phi_5}$ ne peut pas être factorisé. $\overline{\Phi_5}$ est donc **irréductible** sur $\mathbb{F}_2[X]$.

(b) Décomposer Φ_5 en facteurs irréductibles dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$. 1 pt

Solution:

— **Dans** $\mathbb{C}[X]$ **:** Φ_5 est le polynôme dont les racines sont les racines primitives 5-ièmes de l'unité, $\zeta, \zeta^2, \zeta^3, \zeta^4$.

$$\Phi_5(X) = (X-\zeta)(X-\zeta^2)(X-\zeta^3)(X-\zeta^4)$$

— **Dans** $\mathbb{R}[X]$ **:** on apparie les racines conjuguées $\overline{\zeta} = \zeta^4$ et $\overline{\zeta^2} = \zeta^3$.

$$\begin{aligned}\Phi_5(X) &= (X-\zeta)(X-\zeta^4)(X-\zeta^2)(X-\zeta^3) \\ &= \big(X^2 - (\zeta+\zeta^4)X + 1\big)\cdot\big(X^2 - (\zeta^2+\zeta^3)X + 1\big)\end{aligned}$$

Les polynômes quadratiques sont irréductibles sur $\mathbb{R}$ car leurs discriminants sont négatifs :

$$\begin{aligned}D_1 &= (\zeta+\zeta^4)^2 - 4 = (2\cos(2\pi/5))^2 - 4 < 0 \\ D_2 &= (\zeta^2+\zeta^3)^2 - 4 = (2\cos(4\pi/5))^2 - 4 < 0\end{aligned}$$

Ainsi, la décomposition dans $\mathbb{R}[X]$ est :

$$\Phi_5(X) = \big(X^2 - 2\cos(2\pi/5)X + 1\big)\cdot\big(X^2 - 2\cos(4\pi/5)X + 1\big)$$

(c) Démontrer que le polynôme Φ_5 est irréductible dans $\mathbb{Z}[X]$ à l'aide du critère d'Eisenstein. 1,5 pts

Solution: On applique le critère d'Eisenstein au polynôme $\Phi_5(Y+1)$.

$$P(Y) = \Phi_5(Y+1) = \frac{(Y+1)^5 - 1}{(Y+1) - 1} = \frac{Y^5 + 5Y^4 + 10Y^3 + 10Y^2 + 5Y}{Y}$$

$$P(Y) = Y^4 + 5Y^3 + 10Y^2 + 10Y + 5$$

On applique le critère d'Eisenstein avec le nombre premier $p = 5$.

1. Le coefficient dominant est 1, qui n'est pas divisible par $p = 5$.
2. Tous les autres coefficients $(5, 10, 10, 5)$ sont divisibles par $p = 5$.
3. Le terme constant est 5, qui n'est pas divisible par $p^2 = 25$.

$P(Y)$ est irréductible sur $\mathbb{Q}[X]$. Si $\Phi_5(X)$ était réductible, alors $\Phi_5(Y+1) = P(Y)$ serait réductible, ce qui est faux. Φ_5 est donc irréductible sur $\mathbb{Q}[X]$. Puisqu'il est unitaire, il est aussi irréductible sur $\mathbb{Z}[X]$ par le lemme de Gauss.

(d) Démontrer que $\zeta^2 + \zeta^{-2} = (\zeta + \zeta^{-1})^2 - 2$. 0,5 pts

Solution: On développe le terme de droite :

$$\begin{aligned}(\zeta+\zeta^{-1})^2-2 &= \zeta^2+2\cdot\zeta\cdot\zeta^{-1}+(\zeta^{-1})^2-2\\ &= \zeta^2+2\cdot 1+\zeta^{-2}-2\\ &= \zeta^2+\zeta^{-2}\end{aligned}$$

L'identité est vérifiée.

(e) En utilisant le fait que ζ est une racine de Φ_5 et en considérant $\Phi_5(\zeta)/\zeta^2$, déterminer un polynôme de degré 2 qui annule $\cos(2\pi/5)=\frac{1}{2}\big(\zeta+\zeta^{-1}\big)$ sur $\mathbb{Q}$. 1 pt

Solution: Puisque $\Phi_5(\zeta)=0$, on a $\zeta^4+\zeta^3+\zeta^2+\zeta+1=0$. En divisant par ζ^2 (comme $\zeta\neq 0$) :

$$\frac{\Phi_5(\zeta)}{\zeta^2}=\zeta^2+\zeta+1+\zeta^{-1}+\zeta^{-2}=0$$

En regroupant les termes par paire conjuguée et en utilisant la partie (d) :

$$(\zeta^2+\zeta^{-2})+(\zeta+\zeta^{-1})+1=0$$

Posons $u=\zeta+\zeta^{-1}$. On a $\zeta^2+\zeta^{-2}=u^2-2$. L'équation devient :

$$(u^2-2)+u+1=0 \iff u^2+u-1=0$$

On sait que $\cos(2\pi/5)=c=\frac{1}{2}u$, donc $u=2c$. En substituant :

$$(2c)^2+(2c)-1=0 \iff 4c^2+2c-1=0$$

Le polynôme de degré 2 annulant $\cos(2\pi/5)$ sur $\mathbb{Q}$ est $P(X)=4X^2+2X-1$.

(f) Démontrer que ce polynôme est irréductible sur $\mathbb{Q}$ et en déduire l'irrationalité de $\cos(2\pi/5)$. 1 pt

Solution: Soit $P(X)=4X^2+2X-1$.

1. **Irréductibilité sur $\mathbb{Q}$:** $P(X)$ est de degré 2, il est irréductible sur $\mathbb{Q}$ si et seulement s'il n'a pas de racines dans $\mathbb{Q}$. Le discriminant est $\Delta=2^2-4(4)(-1)=4+16=20$. Les racines sont $X=\frac{-2\pm\sqrt{20}}{8}=\frac{-1\pm\sqrt{5}}{4}$. Puisque $\sqrt{5}$ est irrationnel, les racines de $P(X)$ ne sont pas rationnelles. $P(X)$ est **irréductible** sur $\mathbb{Q}$.
2. **Irrationalité de $\cos(2\pi/5)$:** Si $\cos(2\pi/5)$ était rationnel, il serait une racine rationnelle de $P(X)$. Or, $P(X)$ n'a pas de racine rationnelle. Par conséquent, $\cos(2\pi/5)$ est **irrationnel**.

3. On note $\alpha=\sqrt{2}+i\in\mathbb{C}$.
   (a) Déterminer le polynôme minimal P de α sur $\mathbb{R}$. 1 pt

Solution: On cherche $P \in \mathbb{R}[X]$ tel que $P(\alpha) = 0$ et de degré minimal.

$$\alpha - \sqrt{2} = i$$

Élévation au carré :

$$(\alpha - \sqrt{2})^2 = i^2 \implies \alpha^2 - 2\sqrt{2}\alpha + 2 = -1$$

$$\alpha^2 - 2\sqrt{2}\alpha + 3 = 0$$

$P(X) = X^2 - 2\sqrt{2}X + 3$. Les coefficients sont dans $\mathbb{R}$. Puisque α n'est pas réel ($\alpha \notin \mathbb{R}$), son polynôme minimal est de degré ≥ 2. $P(X)$ est de degré 2, il est donc le polynôme minimal.

(b) Déterminer le polynôme minimal Q de α sur $\mathbb{Q}$. Quel lien y a-t-il entre P et Q ? 1,5 pts

Solution: On isole $\sqrt{2}$ dans l'équation précédente :

$$\alpha^2 + 3 = 2\sqrt{2}\alpha$$

Élévation au carré :

$$(\alpha^2 + 3)^2 = (2\sqrt{2}\alpha)^2 \implies \alpha^4 + 6\alpha^2 + 9 = 8\alpha^2$$

$$\alpha^4 - 2\alpha^2 + 9 = 0$$

$Q(X) = X^4 - 2X^2 + 9$. Q est unitaire à coefficients dans $\mathbb{Q}$. On montre que Q est irréductible sur $\mathbb{Q}$ (similaire à Q1.c). $Q(X)$ est le polynôme minimal de α sur $\mathbb{Q}$.
Le lien est que $P(X)$ est un facteur de $Q(X)$ dans $\mathbb{R}[X]$:

$$Q(X) = (X^2 + 3)^2 - 8X^2 = (X^2 + 3 - 2\sqrt{2}X)(X^2 + 3 + 2\sqrt{2}X)$$

$$Q(X) = P(X) \cdot (X^2 + 2\sqrt{2}X + 3)$$

(c) Démontrer que $\mathbb{Q}(\alpha) = \mathbb{Q}(i, \sqrt{2})$. 1 pt

Solution:

1. $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(i, \sqrt{2})$ **:** Puisque $\alpha = \sqrt{2} + i$ et que $\sqrt{2}, i \in \mathbb{Q}(i, \sqrt{2})$, alors $\alpha \in \mathbb{Q}(i, \sqrt{2})$. Comme $\mathbb{Q}(\alpha)$ est le plus petit corps contenant $\mathbb{Q}$ et α, on a l'inclusion.
2. $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\alpha)$ **:** On doit montrer que i et $\sqrt{2}$ sont dans $\mathbb{Q}(\alpha)$. On utilise l'équation :

   $$\alpha^2 - 1 = 2i\sqrt{2} \in \mathbb{Q}(\alpha) \quad \text{et} \quad \alpha = \sqrt{2} + i \in \mathbb{Q}(\alpha)$$

   Plus simplement, on calcule $\alpha^3 + \alpha$:

   $$\alpha = \sqrt{2} + i$$
   $$\alpha^3 = (\sqrt{2} + i)(1 + 2i\sqrt{2}) = 5i - \sqrt{2}$$

$$\alpha^3 + \alpha = (5i - \sqrt{2}) + (\sqrt{2} + i) = 6i$$

Donc $i = \frac{1}{6}(\alpha^3 + \alpha) \in \mathbb{Q}(\alpha)$. De plus, $\sqrt{2} = \alpha - i$. Puisque $\alpha, i \in \mathbb{Q}(\alpha)$, on a $\sqrt{2} \in \mathbb{Q}(\alpha)$.

Les deux inclusions prouvent l'égalité : $\mathbb{Q}(\alpha) = \mathbb{Q}(i, \sqrt{2})$.

(d) Est-ce que $\mathbb{Q}(\alpha)$ est le corps de décomposition de Q sur $\mathbb{Q}$? 0,5 pts

Solution: Oui. Le corps de décomposition K de Q sur $\mathbb{Q}$ est engendré par toutes les racines de Q. Les racines de $Q(X) = X^4 - 2X^2 + 9$ sont $\pm\alpha = \pm(\sqrt{2} + i)$ et $\pm(\sqrt{2} - i)$.

$$K = \mathbb{Q}(\sqrt{2} + i, -(\sqrt{2} + i), \sqrt{2} - i, -(\sqrt{2} - i)) = \mathbb{Q}(\sqrt{2} + i, \sqrt{2} - i)$$

Puisque $i = \frac{1}{2}((\sqrt{2}+i)-(\sqrt{2}-i))$ et $\sqrt{2} = \frac{1}{2}((\sqrt{2}+i)+(\sqrt{2}-i))$, on a $\mathbb{Q}(\sqrt{2}+i, \sqrt{2}-i) = \mathbb{Q}(i, \sqrt{2})$. D'après la partie (c), $K = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\alpha)$. $\mathbb{Q}(\alpha)$ est bien le corps de décomposition de Q sur $\mathbb{Q}$.

(e) Calculer le degré de l'extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ et une base de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$. 1 pt

Solution:

— **Degré de l'extension :** $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\mathrm{Min}_{\mathbb{Q}}(\alpha)) = \deg(Q) = 4$.

— **Base :** Une base est donnée par les puissances de α : $\{1, \alpha, \alpha^2, \alpha^3\}$. Alternativement, en utilisant $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i)$ et la tour d'extensions :

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

Une base est donnée par le produit des bases de $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ($\{1, \sqrt{2}\}$) et de $\mathbb{Q}(i)/\mathbb{Q}$ ($\{1, i\}$) :

$$\mathcal{B} = \{1, i, \sqrt{2}, i\sqrt{2}\}$$

(f) Déterminer le groupe des automorphismes du corps $\mathbb{Q}(\alpha)$. 1 pt

Solution: L'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne de degré 4. Le groupe des automorphismes $G = \mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})$ a donc 4 éléments. Les automorphismes $\sigma \in G$ sont entièrement déterminés par l'image des générateurs i et $\sqrt{2}$.

— $\sigma(i) \in \{\text{racines de } X^2 + 1\} = \{i, -i\}$

— $\sigma(\sqrt{2}) \in \{\text{racines de } X^2 - 2\} = \{\sqrt{2}, -\sqrt{2}\}$

Les 4 automorphismes sont :

$$\sigma_1 : \sigma_1(i) = i, \quad \sigma_1(\sqrt{2}) = \sqrt{2} \quad \text{(identité)}$$
$$\sigma_2 : \sigma_2(i) = -i, \quad \sigma_2(\sqrt{2}) = \sqrt{2} \quad \text{(conjugaison complexe)}$$
$$\sigma_3 : \sigma_3(i) = i, \quad \sigma_3(\sqrt{2}) = -\sqrt{2}$$
$$\sigma_4 : \sigma_4(i) = -i, \quad \sigma_4(\sqrt{2}) = -\sqrt{2}$$

Puisque $\sigma_2^2 = \sigma_3^2 = \sigma_4^2 = \mathrm{id}$, le groupe G est abélien d'ordre 4 où tout élément non trivial est d'ordre 2. Le groupe des automorphismes est isomorphe au **groupe de**

Klein : $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

4. Soit $A = \mathbb{F}_2[X]$ et $I = (X^3 + X + 1)$ l'idéal engendré par $P = X^3 + X + 1$ dans A.

(a) Démontrer que P est irréductible dans A. 1 pt

Solution: $P = X^3 + X + 1$ est de degré 3. Il est réductible dans $\mathbb{F}_2[X]$ si et seulement s'il possède une racine dans $\mathbb{F}_2$.
- $P(0) = 0^3 + 0 + 1 = 1 \neq 0$.
- $P(1) = 1^3 + 1 + 1 = 3 \equiv 1 \pmod 2 \neq 0$.

Puisque P n'a pas de racine dans $\mathbb{F}_2$, il est **irréductible** dans $A = \mathbb{F}_2[X]$.

(b) Démontrer que le quotient A/I est un corps. 0,5 pts

Solution:
- L'anneau $A = \mathbb{F}_2[X]$ est un anneau principal (car $\mathbb{F}_2$ est un corps).
- Dans un anneau principal, un idéal $I = (P)$ est maximal si et seulement si le générateur P est irréductible.
- D'après la partie (a), $P = X^3 + X + 1$ est irréductible.

L'idéal I est donc maximal, et par conséquent, le quotient A/I est un **corps**.

(c) Quel est le cardinal de ce corps ? 1 pt

Solution: Les éléments de $A/I = \mathbb{F}_2[X]/(P)$ sont représentés par les polynômes de degré strictement inférieur au degré de P, soit 3. Les éléments sont de la forme $a_2X^2 + a_1X + a_0$, avec $a_0, a_1, a_2 \in \mathbb{F}_2$. Chaque coefficient a_i a 2 choix possibles (0 ou 1). Le cardinal est $2 \times 2 \times 2 = 2^3 = 8$.

(d) Quel est l'inverse de l'élément $[X] \in A/I$? 1,5 pts

Solution: Soit $\alpha = [X] \in A/I$. Par définition, α est une racine de P, donc $\alpha^3+\alpha+1 = 0$. Dans $\mathbb{F}_2[X]$, $1 = -1$, donc l'équation s'écrit :

$$\alpha^3 + \alpha = 1$$

En factorisant α à gauche :

$$\alpha(\alpha^2 + 1) = 1$$

L'inverse de $\alpha = [X]$ est $\alpha^{-1} = \alpha^2 + 1$. L'inverse est l'élément $[X^2 + 1]$.